Detail Matrix of Federal Law and Policy That Parallels the ISE Privacy and Civil Liberties Implementation Guide Process

Background:

Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Section 1 of Executive Order 13388 ("Further Strengthening the Sharing of Terrorism Information to Protect Americans") provides that, "[t]o the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information among agencies … [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …." Guidelines for the implementation of these requirements were developed at the President's direction by the Attorney General and the Director of National Intelligence, in coordination with the heads of executive departments and agencies (agencies) that possess or use intelligence or terrorism related information in the ISE. The ISE Privacy Guidelines were approved by the President and issued by the Program Manager for the ISE (PM-ISE) on December 4, 2006.

The ISE Privacy Guidelines require agencies to identify applicable privacy laws, regulations, policies, and other authorities to determine whether policies and procedures are in place for all protected information in the ISE, identify gaps, and formulate any policies or procedures required to fill the gaps. Many agencies have already completed the bulk of these activities in the course of complying with cross-cutting federal laws and policies.

To assist agencies with leveraging work already conducted in these areas, the ISE Privacy Guidelines Committee has reviewed five federal authorities with broad applicability to information sharing by federal agencies and identified requirements that are similar or identical to those required by the ISE Privacy Guidelines. These authorities are:

- The Privacy Act of 1974
- The Privacy Management Report, as required under the implementation guidelines for the Federal Information Security Management Act of 2002 (FISMA)
- OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 26, 2003)
- OMB Memorandum 06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006)
- OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007)

This Matrix is offered to federal agencies participating in the ISE as an aid to addressing the requirements of the ISE Privacy Guidelines. It is not intended to be comprehensive, and most agencies are subject to additional privacy-related authorities that they may also leverage in order to develop their ISE privacy protection plan.

Table I. Comparison of ISE Privacy and Civil Liberties Implementation Guide to Cross-Cutting Federal Agency Requirements

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
1	2 of 6	**Identify** any applicable laws, Executive Orders, policies, and procedures that apply to protected information that the agency will make available or access through the ISE (ISE Privacy Guidelines, Section 2 (a and b)).	Consider: Rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records or in maintaining any record (as required to be promulgated per Section 552a(e)(9)). Rules providing for individual notification, access, redress, disclosure, review, and fees (as required to be promulgated per Section 552a(f)(1) through (f)(5)). Computer Matching Agreements executed pursuant to Section 552a(0).	Consider: FISMA Section D requirement that agencies maintain a written process for determining whether a PIA is needed and conducting a PIA. FISMA Section D requirement that agencies maintain a written process for determining continued compliance with stated Web privacy policies.		Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
1	2 of 6	Consider including terrorism-related information sharing practices that may be more informal, as well as any proposed terrorism-related information sharing plans in documentation.	Consider: Any rules promulgated to permit exemptions for certain systems to the "no disclosure without consent" rule, notably the law enforcement exemption under 553a(b)(7) (permitting disclosure "to another agency or to an instrumentality of any governmental			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity...." See full citation at 553a(b)(7)).			required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
1	2 of 6	Identify collection (acquisition and access) laws, Executive Orders, policies, and procedures.	Consider: Rules established to permit collections of information, such as those setting policies for creating systems of records, which must address the collection of information, methods by which it is collected, formal notifications to individuals whose information is solicited regarding authority and purposes of collection, controls ensuring the timeliness, relevance, and accuracy of information, establishment of safeguards and security controls, and disclosure practices (5 U.S.C. 552a(e)). Documented access procedures for individuals to request and review information pertaining to them			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			according to 5 U.S.C. 552a(d), (j), and (k).			identifiable information, all under OMB Memorandum 07-16.
1	2 of 6	Identify retention (storage, safeguarding, and validation) laws, Executive Orders, policies, and procedures.	Consider: Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of records (5 U.S.C. 552a(e)(4)(E).			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15.
1	2 of 6	Identify production (dissemination and publication) laws, Executive Orders, policies, and procedures.	Consider: Rules propagated to ensure that records are accurate, complete, timely, and relevant for agency purposes prior to disclosure (5 U.S.C. 552a(e)(6)). Rules propagated to ensure that disclosures of records contained in systems of records are made only pursuant to a written request by or with the prior written consent of the individual to whom the record pertains, unless disclosure of the record falls under one of the 12 exceptions to the Privacy Act (including disclosures related to		For each PIA, agencies must consider why the information is being collected. See OMB 03-22, Section C.1.a.ii. Comprehensive PIAs may therefore reflect the legal authority for the information collection.	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			the law enforcement exception at 5 U.S.C. 552a(b)(7). Rules propagated to ensure agencies retain records of disclosures per 5 U.S.C. 552a(c).			notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
1	2 of 6	Identify use (action and response taken upon receipt of such information) laws, Executive Orders, policies, and procedures.	Consider: Rules propagated to ensure that agencies indicate purpose and routine use of information within systems of records notices (5 U.S.C. 552a(e)(4)).		For each PIA, agencies must describe the intended use of the information being collected. See OMB 03-22, Section C.1.a.iii.	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15, including "procedures and restrictions on the use or removal of personally identifiable information beyond agency premises or control." Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
1	2 of 6	Identify sharing (dissemination of terrorism information among ISE participants) laws, Executive Orders, policies, and procedures.	Consider: Rules propagated to reflect that requirements of computer matching programs do not apply to matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel (5 U.S.C. 552a(a)(8)(B)(vi)).		For each PIA, agencies must describe with whom the information will be shared (e.g., another agency for a specified programmatic purpose). See OMB 03-22, Section C.1.a.iv.	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
1	2 of 6	Identify management (oversight and governance of the above practices and processes) laws, Executive Orders, policies, and procedures.	Consider: Rules propagated to ensure agencies maintain an appropriate Data Integrity Board to oversee and coordinate Computer Matching Agreements, per 552a(u).	The report asks agencies to identify a Senior Agency Official for Privacy and demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy).		Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	**Assess** and identify gaps between existing protections and the protections identified in the ISE Privacy Guidelines.		Consider: FISMA Section D requirement for agencies to provide documentation demonstrating corrective actions planned, in progress, or completed to remedy identified compliance deficiencies (in		Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy, including the requirement to "take corrective action as appropriate to ensure your agency has adequate

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
				reference to privacy laws and guidelines).		safeguards to prevent the intentional or negligent misuse of or unauthorized access to personally identifiable information," required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Determine and document agency-wide information privacy and civil liberties policies, procedures, guidelines, and practices.				
2	3 of 6	Agencies should work with affected agency components to determine and document the agency's privacy and civil liberties legal and policy environment for				

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		terrorism information sharing.				
2	3 of 6	Agencies should review what legal authorities are controlling or relevant.				
2	3 of 6	Agencies should review what information may or may not be collected.	The Act requires agencies to maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President; collect information, to the greatest extent practicable, directly from the subject individual when information could result in adverse determinations about an individual's rights, benefits, and privileges under federal programs; and include justification and use of information collected directly from the individual as indicated within individual and federal notice statements, unless exempted under 5 U.S.C. 552a(j) or (k) (5 U.S.C. 552a(e)(1-3)).			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15, including ensuring that "agency employees are reminded within the next 30 days of their specific responsibilities... acquiring and using" personally identifiable information. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						information, all under OMB Memorandum 07-16.
2	3 of 6	Agencies should review how information can be collected.	The Act requires agencies to maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President; collect information, to the greatest extent practicable, directly from the subject individual when information could result in adverse determinations about an individual's rights, benefits, and privileges under federal programs; and include justification and use of information collected directly from the individual as indicated within individual and federal notice statements, unless exempted under 5 U.S.C. 552a(j) or (k). (5 U.S.C. 552a(e)(1-3)).			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15, including ensuring that "agency employees are reminded within the next 30 days of their specific responsibilities... acquiring and using" personally identifiable information. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Agencies should review eligible parties (internal and external) to receive information that is collected.	The Privacy Act does not put restriction on the parties eligible to receive a Privacy Act record. Agencies must, however, ensure that information is disclosed pursuant to a written request by or with the prior consent of the individual to whom the record pertains, unless disclosure of the record is made according to one of 12 exemptions (5 U.S.C. 552a(b)). Though agencies must also consider the requirements around "matching programs," matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel or matches for the purposes of enforcing criminal laws are exempt from specific requirements related to "matching			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			programs" (5 U.S.C. 552a(a)(8)(B)(vi)). In addition, exemptions to the Privacy Act may result in information being withheld for law enforcement or investigative purposes (5 U.S.C. 552a(j) and (k)).			
2	3 of 6	Agencies should review their transparency policies.	Agencies are required to post a system of records notice in the *Federal Register* for information collections subject to the Privacy Act. The notice should detail information about the system of records (5 U.S.C. 552a(e)(4)).		For each PIA, agencies must describe what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses) and how individuals can grant consent. See OMB 03-22, Section C.1.a.v.	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15.

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
2	3 of 6	Agencies should review their redress policies.	Agencies must have specific policies and procedures in place for members of the public to view and amend records about them held by the agency (5 U.S.C. 552a (f)(3-5)). Agencies may be exempted from providing access to records if the records meet certain law enforcement and investigative exemptions (5 U.S.C. 552a(j) and (k)).		For each PIA, agencies must describe what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses) and how individuals can grant consent. See OMB 03-22, Section C.1.a.v.	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Agencies should review their accountability, enforcement, and training policies.	Each agency that maintains a system of records shall establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records or in maintaining any record and instruct each such person with respect to such rules and the requirements of this section, including any other rules and	The report asks respondents to indicate by component (e.g., bureau, agency) whether the agency has a training program to ensure that all agency personnel are generally familiar with		Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15, including ensuring that "agency employees are

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			procedures adopted pursuant to this section and the penalties for noncompliance (552a(e)(9)). This requirement extends to contractors as well as other agency employees (552a(m)).	information privacy laws, regulations, and policies and understand the ramifications of inappropriate access and disclosure and, in particular, whether training for the following programs were reviewed in the previous fiscal year: Section M Contracts, Records, Practices, Routine Uses, Exemptions, Matching Programs, Training Violations, Systems of Records.		reminded...of their specific responsibilities for safeguarding personally identifiable information and the rules for acquiring and using such information, as well as the penalties for violating these rules." Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Work with agency components to determine agency-wide information privacy and civil liberties policies, procedures, guidelines, and practices.				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Review whether or not the Fair Information Principles are employed.				
2	3 of 6	Review which records are Privacy Act versus non-Privacy Act records.	The Privacy Act defines records as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph" (5 U.S.C. 552a(a)(4)).	Pursuant to OMB Circular A-130, agencies must conduct reviews and document their inventory of Privacy Act System of Records Notices (SORNs).	For each PIA, agencies must determine whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a. See OMB 03-22, Section C.1.a.vii.	
2	3 of 6	Review "minimum necessary" information sharing policies, procedures, guidelines, and practices.	The Privacy Act requires each agency that holds a system of records to maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President (5 U.S.C. 552a(e)(1)).			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						access personally identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Review limitations on redisclosure policies, procedures, guidelines, and practices.	The Privacy Act must collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs (5 U.S.C. 552a(e)(2)). In addition, agencies must ensure that information is disclosed pursuant to a written request by or with the prior consent of the individual to whom the record pertains, unless disclosure of the record is made according to one of 12 exemptions (5 U.S.C. 552a(b)).			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
2	3 of 6	Review any alerts as to the reliability of the information.	Agencies maintaining a system of records must "establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section" (5 U.S.C. 552a(f)(4)). In the event that an individual, whose record is maintained by an agency, requests an amendment to the information that they believe to be inaccurate, irrelevant, untimely, or incomplete, the agency must promptly make the correction or inform the individual of its refusal to amend the record. Agencies that fail "to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of or			

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual" are subject to civil penalties (5 U.S.C. 552a(g)(1)(C)).			
2	3 of 6	Review policies, procedures, guidelines, and practices around monitored disclosure.				Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Review information retention practices.	Agencies must indicate within their system of records notices (SORN) the retention and disposal policies and procedures in place for the information collection (5 U.S.C. 552a(e)(4)(E)).			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memoranda 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
2	3 of 6	Review information security controls.	Agencies must indicate within their SORN the appropriate storage, retrievability, and access control safeguards in place for the information collection (5 U.S.C. 552a(e)(4)(E)).		For each PIA, agencies must describe how the information will be secured (e.g., administrative and technological controls). See OMB 03-22, Section C.1.a.vi.	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15, including ensuring the agency "has adequate safeguards to prevent the intentional or negligent misuse of or unauthorized access to personally identifiable information. This review shall address all administrative, technical, and physical means used by your agency to control such information...." Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						identifiable information, all under OMB Memorandum 07-16.
2	3 of 6	Assess how commercial data (information obtained from a commercial source) is collected or stored and used.				
2	3 of 6	Assess whether commercial data sharing arrangement protections are applied.				
2	3 of 6	Assess whether commercial data has assurances on reliability applied.				
2	3 of 6	Assess whether commercial data has sharing alerts applied.				
2	3 of 6	Assess whether commercial data has verification requirements applied.				

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
2	3 of 6	Agencies may find it useful to identify or create a policy manual or comprehensive repository of all privacy and civil liberties policies and procedures necessary for documenting consistency with the ISE Privacy Guidelines.		Agencies must document current documentation demonstrating review of compliance with information privacy laws, regulations and policies, along with dates the documentation was created. Consider FISMA Section D request for supplying a compilation of the agency's privacy and data protection policies and procedures to the agency's IG.		Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	4 of 6	Use the "As-Is" state data to compare what is required by the ISE Privacy Guidelines (the "To-Be" state).				Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy, including the requirement to "take corrective action as appropriate to ensure your agency has adequate safeguards to prevent the intentional or negligent misuse of or unauthorized access to

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						personally identifiable information," required by OMB Memorandum 06-15. This previous gap analysis and corrective action activity may address many of the requirements of the ISE Privacy Guidelines. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	4 of 6	Identify areas where no privacy and civil liberties policy or procedure exists.				
2	4 of 6	Identify areas where privacy and civil liberties policy or procedures are not adhered to.		Agencies must report whether they maintain documentation demonstrating review of compliance with information privacy laws, regulations, and policies		

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
				and provide the date the documentation was created.		
2	4 of 6	Identify areas where privacy and civil liberties policy or procedures are misunderstood or lack implementation guidance.		Agencies must report whether they maintain documentation demonstrating review of compliance with information privacy laws, regulations, and policies and provide the date the documentation was created.		
2	4 of 6	Identify areas where existing privacy and civil liberties policy, procedures, or practices are insufficient to address the ISE Privacy Guidelines requirements.				
2	4 of 6	Identify areas where training regarding privacy and civil liberties policy and procedures does not sufficiently address the ISE Privacy Guidelines requirements.		The report asks respondents to indicate by component (e.g., bureau, agency) whether the agency has a training program to ensure that all agency personnel are generally familiar with information privacy laws, regulations,		

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
				and policies and understand the ramifications of inappropriate access and disclosure and, in particular, whether training for the following programs was reviewed in the previous fiscal year: Section M Contracts, Records, Practices, Routine Uses, Exemptions, Matching Programs, Training Violations, Systems of Records.		
2	4 of 6	Consider whether the agency seeks and retains only what it is permitted to collect and retain.	Agencies maintaining a system of records must "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President" (5 U.S.C. 552a(e)(1)). Agencies must have procedures in place for the retention and disposal of information collected in a system of records, and must be detailed in the system of records notice (5 U.S.C. 552a(e)(4)). (Note: this is subject to exemption			

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			under section (j) and (k) of 5 U.S.C. 552a.)			
2	4 of 6	Consider whether data is only collected lawfully.	The Privacy Act requires that each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President (552a(e)(1)).			
2	4 of 6	Identify interagency rules that impede sharing without protecting privacy, and identify what purpose each restriction is designed to serve.	The Privacy Act contains numerous exemptions from compliance for agencies involved in counter-intelligence, criminal law enforcement, and background investigation efforts.			
2	4 of 6	Raise issue of impeding interagency rules with the Privacy Guidelines Committee.				
2	4 of 6	Ensure that information identified within the ISE and shared via ISE processes is used consistent with the provisions of Executive Order				

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		13388, for the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States.				
3	5 of 6	Ensure that all protected information in the ISE is covered by applicable privacy policies.				
3	5 of 6	Document that existing laws, Executive Orders, policies, and procedures are in compliance with the ISE Privacy Guidelines.				
3	5 of 6	Develop new policies to fill any gaps, and bring the agency into compliance with the ISE Privacy Guidelines.				Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy, including the requirement to "take corrective action as appropriate to ensure your agency has adequate safeguards to prevent the intentional or negligent misuse of or unauthorized access to personally identifiable

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						information," required by OMB Memorandum 06-15. This previous gap analysis and corrective action activity may address many of the requirements of the ISE Privacy Guidelines. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 6	Agencies must have a written ISE privacy protection policy stating that protected information shall be shared among agencies, organizations, and other persons only as allowed by the agency's information sharing policy and guidelines collected in a manual or held in a central repository.				

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
3	5 of 6	Agencies must have protocols and guidelines that define categories of information that may be shared.				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 6	Agencies must have protocols and guidelines that define categories of entities with which data may be shared, with restrictions for each (law enforcement agencies, intelligence agencies, commercial entities, individuals who are the subjects of records, etc.).	The Privacy Act covers federal interagency, and agency-to-individual disclosure practices, with specific requirements and exemptions for each. The Privacy Act does not make any explicit distinctions for requirements for sharing information with commercial entities. Agencies should review the exemptions contained within the Privacy Act for information supporting criminal law enforcement and counter-intelligence operations.			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 6	Agencies must have protocols and guidelines that determine information sharing sources (e.g.,				Consider: Policies required to be drafted relating privacy breach notification, including reviews

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		systems of records/databases).				of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 6	Agencies must have protocols and guidelines that determine information sharing methods (e.g., software applications or other media).				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 6	Agencies must have protocols and guidelines that determine how sharing requests may be received.	The Privacy Act requires agencies to ensure that information is disclosed pursuant to a disclosed routine use to a written request by or with the prior consent of the individual to whom the record pertains, or according to one of 12 exemptions (5 U.S.C. 552a(b)).			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 6	Agencies must have protocols and guidelines that determine what processing must be conducted prior to sharing (formatting, redaction, review, etc.).	Prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to (b)(2) of 5 U.S.C. 552a, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant for agency purposes (5 U.S.C. 552a(e)(6)). In addition, exemptions listed in (j) and (k) of 5 U.S.C. 552a may require additional review and redaction of information contained in the record.			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 6	Agencies must have protocols and guidelines that determine information sharing protocols (encryption, deidentification/ anonymization, documentation, and auditing).				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						Memorandum 07-16.
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding identity and authorities of information requester/receiver and sender.	Agencies must establish matching agreements for all matching programs detailing authority of information collection; justification for the matching program; description of records to be matched; and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o).			
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding required privacy and civil liberties protections (encryption, limited-use agreements, data retention, notice and consent of data subjects where applicable, minimum necessary data shared).	Agencies must establish matching agreements for all matching programs detailing authority of information collection; justification for the matching program; description of records to be matched; and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o).			
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding required security protections	Agencies must establish matching agreements for all matching programs detailing authority of information collection; justification for the matching program; description of		For each PIA, agencies must describe how the information will be secured (e.g., administrative and	

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		(firewalls, intrusion detection systems, physical security, training and awareness of staff, authorization and authentication, etc.).	records to be matched; and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o).		technological controls). See OMB 03-22, Section C.1.a.vi.	
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding dispute resolution process				
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding rights in data, if applicable.				
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding limitations on redisclosure.	Agencies must establish matching agreements for all matching programs detailing authority of information collection; justification for the matching program; description of records to be matched; and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o).			
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding effects of laws and regulations (including	Agencies must establish matching agreements for all matching programs detailing authority of information collection; justification for the matching program; description of records to be matched;			

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		exemptions therefrom).	and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o).			
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding disclaimers of warranties/ assurances of accuracy.	Agencies must establish matching agreements for all matching programs detailing authority of information collection; justification for the matching program; description of records to be matched; and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o).			
3	5 of 6	Agencies must have Memoranda of Understanding (MOU), including terms and requirements regarding monitoring/auditing responsibilities of sender and receiver (methods, frequency, roles and responsibilities, remediation).				
3	5 of 6	New or existing policies should include an overarching policy for the periodic and careful review of agency and personnel compliance with privacy and civil liberties procedures (such as through an				Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		inspection/review process).				15.
3	6 of 6	New or existing policies should include an overarching mechanism for promptly reporting noncompliance with all ISE privacy and civil liberties procedures.				
3	6 of 6	New or existing policies should include an overarching mechanism for responding to incidents of noncompliance, including sanctions for individuals that are negligently or willfully noncompliant.	The Privacy Act stipulates civil and criminal penalties for agencies failing to comply with the provisions of the Privacy Act (5 U.S.C. 552a(g) and (h)).			
3	6 of 6	New or existing policies should include policies on computer matching and other data merges, including implications of the Privacy Act.	Agencies must consider the requirements around "matching programs," as defined in the Privacy Act. All matching programs must have a matching agreement in place that details the authority of information collection; justification for the matching program; description of records to be matched; and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o).			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15, including a requirement to ensure "agency employees are reminded within the next 30 days of their specific responsibilities for safeguarding

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			Matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of federal personnel or federal contractor personnel or matches for the purpose of enforcing criminal laws are exempt from specific requirements related to "matching programs" (5 U.S.C. 552a(a)(8)(B)(vi)). Agency Data Integrity Boards are responsible for reviewing and approving all new and existing matching agreements annually and reporting to the Office of Management and Budget.			personally identifiable information, the rules for acquiring and using such information *as well as the penalties for violating these rules* [emphasis added]."
3	6 of 6	New or existing policies should include posting of Systems of Record Notices (SORNs) and other Privacy Act requirements, if applicable.	The Privacy Act requires agencies to develop and post Systems of Records Notices in the *Federal Register* (5 U.S.C. 552a(e)(4).			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
3	6 of 6	New or existing policies should include data accuracy, completeness, and timeliness controls.	The Privacy Act contains requirements for agencies to maintain procedures for ensuring data accuracy, completeness, relevance, and timeliness. In addition, agencies must ensure accuracy, completeness, relevance, and timeliness of information prior to disseminating/disclosing information.			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	6 of 6	Agencies developing new policies/procedures should address relevant Federal laws, regulations, guidelines, interagency agreements or rules, or other agency-specific directives driving each requirement, especially those restricting data sharing.	Agencies must consider the requirements around "matching programs," as defined in the Privacy Act. All matching programs must have a matching agreement in place that details the authority of information collection; justification for the matching program; description of records to be matched; and procedures for notification, redress, information retention, redisclosure, and assessment of information accuracy (5 U.S.C. 552a(o). Matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of federal personnel or			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			federal contractor personnel or matches for the purposes of enforcing criminal laws are exempt from specific requirements related to "matching programs" (5 U.S.C. 552a(a)(8)(B)(vi)). Agency Data Integrity Boards are responsible for reviewing and approving all new and existing matching agreements annually and reporting to the Office of Management and Budget.			
3	6 of 6	Agencies developing new policies/procedures should address the specific mandatory required action or end state.				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	6 of 6	Agencies developing new policies/procedures should address any exemptions to each requirement that the agency may invoke or has invoked, if				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy;

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		applicable.				incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	6 of 6	Agencies developing new policies/procedures should address the specific officials and personnel affected by the policies and those responsible for implementation and oversight.				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	6 of 6	Agencies developing new policies/procedures should address the particular detailed procedures to be followed by each category of affected staff, including enforcement and assurance responsibilities.				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to

STAGE I						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						access personally identifiable information, all under OMB Memorandum 07-16.

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
1	2 of 5	**Identify** the terrorism information systems, sharing arrangements, and "protected information" that are currently being shared or could be shared in the ISE.				
1	2 of 5	Agencies will need to identify existing systems and databases that contain terrorism information (personally identifiable information currently shared by law or agency policy, including interagency memoranda of agreement or other sharing arrangements). (Note: If agencies already have a process that covers this step, they do not need to do additional assessments of those systems solely for the purpose of the ISE Privacy Guidelines.)				
1	2 of 5	Agencies will need to identify existing systems and databases that contain terrorism information that will potentially be shared through the ISE. (Note: If agencies already have a process that covers this step,				

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		they do not need to do additional assessments of those systems solely for the purpose of the ISE Privacy Guidelines.)				
1	2 of 5	Agencies should analyze the Green Pages to ensure that systems of records/databases are appropriately identified as Category I.				
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category I systems and databases contained within the Green Pages.				
1	2 of 5	Agencies should identify their systems of records/databases that are clearly Category I, although not identified in the Green Pages.				
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category I systems and databases not contained in the Green Pages.				
1	2 of 5	Agencies should identify their Category II systems				

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		of records/databases that contain a mix of terrorism and nonterrorism information.				
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category II systems and databases.				
1	2 of 5	Agencies should identify their Category III systems of records/databases that contain information that is clearly not terrorism information but that may become subject to ISE sharing as part of a terrorism investigation.				
1	2 of 5	Agencies should identify any information sharing agreements and other arrangements that exist or are planned for Category III systems and databases.				
1	2 of 5	For Category II and III systems of records/databases, identify the risk environment around those containing PII terrorism information to determine whether special protections are warranted.				

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
1	3 of 5	To identify the risk environment for systems of records/databases, determine whether the system of record/database contains sensitive information that is subject to privacy and civil liberties protections (e.g., personally identifiable information that reveals medical, financial, or religious information).			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment for systems of records/databases, determine what specific protections each category of information must receive under legal, regulatory, or contractual obligations.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment for systems of records/databases, determine what information privacy policies and practices are applied.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems.	

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
					See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment, determine whether privacy protection exemptions assigned to the data or system apply if the information is shared within the ISE.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment, determine the likelihood that the data will be shared within the ISE.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment, determine how each category of information under consideration could be exploited if it were inappropriately disclosed, accessed, or intercepted.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk	

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
					assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment, determine what harms would result to the individual if information were inappropriately disclosed, accessed, or intercepted.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment, determine the magnitude of the harms that would result—to the individual, the organization, or to larger interests such as those of the United States—if information were inappropriately disclosed, accessed, or intercepted.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
1	3 of 5	To identify the risk environment, determine what types of persons would be interested in inappropriately accessing, transmitting, or			PIAs must address risk assessments conducted during the system development life cycle, with	

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		receiving each type of information, both inside and outside of the agency maintaining it.			special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
2	4 of 5	**Assess** and identify the risk to privacy and civil liberties for the terrorism systems, identified in Step 1.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
2	4 of 5	Assess whether the agency's risk assessment criteria was applied to determine whether ISE information shared in the ISE should continue to be shared and, if so, whether special protections are warranted.			PIAs must address risk assessments conducted during the system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
2	4 of 5	Assess whether the agency's risk assessment criteria (for application to determine whether			PIAs must address risk assessments conducted during the	

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		ISE information under consideration for sharing in the ISE) was applied to determine whether the information should be shared in the ISE and, if so, whether special protections are warranted.			system development life cycle, with special attention given to risk assessments conducted for major systems. See Section C.2.a.i.1 and C.2.a.ii.3.	
2	4 of 5	Agencies must assess their implementation of laws and policies to identified systems.				Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their information privacy and civil liberties marking system that ensures information is handled in accordance with applicable legal requirements is applied to ISE information. (Refer	The Privacy Act requires that all categories of information collected are specified within a System of Records Notice (SORN), and in a statement at the point of collection (5 U.S.C. 552a(e)(3).			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy, and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
		to Notice Mechanisms.)				notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their data quality procedures designed to ensure accuracy, timely correction, and appropriate retention of data are applied to ISE information. (Refer to Data Quality.)	The Privacy Act requires agencies to ensure that records are accurate, complete, timely, and relevant for agency purposes prior to disclosure (5 U.S.C. 552a(e)(6)).			Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy, and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
						16.
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their data security procedures designed to safeguard protected information are applied to ISE information. (Refer to Data Security.)	Agencies must indicate within their system of records notices the appropriate storage, retrievability, and access control safeguards in place for the information collection (5 U.S.C. 552a(e)(4)(E)).		For each PIA, agencies must describe how the information will be secured (e.g., administrative and technological controls). See OMB 03-22, Section C.1.a.vi.	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy, and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their auditing procedures designed to hold personnel accountable, ensure training of staff, and conduct reviews and audits designed to obtain and verify compliance are applied to ISE information? (Refer to Accountability.)	Each agency that maintains a system of records shall establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records or in maintaining any record and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance (552a(e)(9)). This requirement extends to contractors as well as other agency employees (552a(m)).	The report asks respondents to indicate by component (e.g., bureau, agency) whether the agency has a training program to ensure that all agency personnel are generally familiar with information privacy laws, regulations, and policies and understand the ramifications of inappropriate access and disclosure and, in particular, whether training for the following programs was reviewed in the previous fiscal year: Section M Contracts, Records, Practices, Routine Uses, Exemptions, Matching Programs, Training Violations, Systems of Records.		Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy, and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
2	4 of 5	To assess application of laws and policies to systems, agencies must assess whether their transparency and redress procedures designed to inform the public of agency information and privacy policies and address complaints from persons regarding information under agency control are in place for the ISE. (Refer to Redress.)	Agencies maintaining a system of records must "establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section" (5 U.S.C. 552a(f)(4)). In the event that an individual whose record is maintained by an agency requests an amendment to the information that the individual believes to be inaccurate, irrelevant, untimely, or incomplete, the agency must promptly make the correction or inform the individual of its refusal to amend the record. Agencies that fail "to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or	The report asks respondents to indicate by component (e.g., bureau, agency) whether the agency has a training program to ensure that all agency personnel are generally familiar with information privacy laws, regulations, and policies and understand the ramifications of inappropriate access and disclosure and, in particular, whether training for the following programs was reviewed in the previous fiscal year: Section M Contracts, Records, Practices, Routine Uses, Exemptions, Matching Programs, Training Violations, Systems of Records.		Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15.

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
			benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual" are subject to civil penalties (5 U.S.C. 552a(g)(1)(C)).			
3	5 of 5	**Protect** by establishing actions that the agency needs to take for "protected information" shared from those identified systems.	Agencies must indicate within their SORN the appropriate storage, retrievability, and access control safeguards in place for the information collection (5 U.S.C. 552a(e)(4)(E)).			
3	5 of 5	Document agency's protections required for specific systems/ information shared in the ISE based on assessment of systems and policy requirements.		Agencies must indicate whether they have a written process for (a) determining whether a PIA is needed, and (b) conducting a PIA.	Agencies are required to conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available. This requirement applies to all executive branch departments and agencies	Consider: Results of the review of privacy policies and processes conducted by the agency's Senior Official for Privacy and corrective actions, required by OMB Memorandum 06-15. Policies required to be drafted relating privacy breach notification, including reviews of general privacy

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
					(“agencies”) and their contractors that use information technology or that operate Web sites for purposes of interacting with the public.	and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 5	If existing policies or procedures address the required provision, an agency must document that an existing policy or procedure complies with the ISE Privacy Guidelines provision.				
3	5 of 5	Agencies should put in place a policy that implements required protections for the system.	Agencies must indicate within their SORN the appropriate storage, retrievability, and access control safeguards in place for the information collection (5 U.S.C. 552a(e)(4)(E)).			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
3	5 of 5	Agencies should put in place reporting/notification procedures regarding violations of agency-protection policies, as appropriate, that address reporting, investigating, and responding to such violations.	The Privacy Act stipulates civil and criminal penalties for agencies failing to comply with the provisions of the Privacy Act (5 U.S.C. 552a(g) and (h)).			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.
3	5 of 5	Agencies should put in place audit and enforcement mechanisms for the system as required by policy for that system.	The Privacy Act stipulates civil and criminal penalties for agencies failing to comply with the provisions of the Privacy Act (5 U.S.C. 552a(g) and (h)).			Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
3	5 of 5	Agencies should provide training for personnel authorized to share protected information for the system regarding the agency's requirements and policies for collection, use, and disclosure of protected information and as appropriate for reporting violations of agency privacy and civil liberties protection policies.	Each agency that maintains a system of records shall establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records or in maintaining any record and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance (552a(e)(9)). This requirement extends to contractors as well as other agency employees (552a(m)).	The report asks respondents to indicate by component (e.g., bureau, agency) whether the agency has a training program to ensure that all agency personnel are generally familiar with information privacy laws, regulations, and policies and understand the ramifications of inappropriate access and disclosure and, in particular, whether training for the following programs was reviewed in the previous fiscal year: Section M Contracts, Records, Practices, Routine Uses, Exemptions, Matching Programs, Training Violations, Systems of Records.		Consider: Policies required to be drafted relating privacy breach notification, including reviews of general privacy and security policy; incident reporting and handling; external breach notification; and the responsibilities of individuals authorized to access personally identifiable information, all under OMB Memorandum 07-16.

STAGE II						
Step	**Page Number**	**ISE Privacy and Civil Liberties Implementation Guide**	**Privacy Act**	**FISMA PMR**	**OMB M-03-22**	**OMB M-06-15, M-07-16**
3	5 of 5	Agencies should ensure cooperation with audits and reviews by officials with responsibility for providing oversight with respect to the ISE.				
3	5 of 5	Agencies should ensure that the agency's designated ISE privacy official receives reports (or copies) regarding alleged errors in protected information that originates from the agency.				